

Improved Uncertainty Relation in the Presence of Quantum Memory

Yunlong Xiao,^{1,2} Naihuan Jing*,^{3,4} Shao-Ming Fei,^{5,2} and Xianqing Li-Jost²

¹*School of Mathematics, South China University of Technology, Guangzhou, Guangdong 510640, China*

²*Max Planck Institute for Mathematics in the Sciences, 04103 Leipzig, Germany*

³*Department of Mathematics, Shanghai University, Shanghai 200436, China*

⁴*Department of Mathematics, North Carolina State University, Raleigh, NC 27695, USA*

⁵*School of Mathematical Sciences, Capital Normal University, Beijing 100048, China*

Berta *et al.*'s uncertainty principle in the presence of quantum memory [M. Berta *et al.*, Nat. Phys. **6**, 659 (2010)] reveals uncertainties with quantum side information between the observables. In the recent important work of Coles and Piani [P. Coles and M. Piani, Phys. Rev. A **89**, 022112 (2014)], the entropic sum is controlled by the first and second maximum overlaps between the two projective measurements. We generalize the entropic uncertainty relation in the presence of quantum memory and find the exact dependence on all d largest overlaps between two measurements on any d -dimensional Hilbert space. Our bound is rigorously shown to be strictly tighter than previous entropic bounds in the presence of quantum memory, which have potential applications to quantum cryptography with entanglement witnesses and quantum key distributions.

PACS numbers: 03.65.Ta, 03.67.-a, 42.50.Lc

Heisenberg's uncertainty principle [1] plays a central role in physics and marks a distinguished characteristic of quantum mechanics. The principle bounds the uncertainties of measurement outcomes of two observables, such as the position and momentum of a particle. This shows the underlying difference of quantum mechanics from classical mechanics where any properties of a physical object can be quantified exactly at the same time. In Robertson's formulation [2], the product of the standard deviations (denoted by $\Delta(R)$ for the observable R) of the measurement of two observables R and S is controlled by their commutator:

$$\Delta R \Delta S \geq \frac{1}{2} |\langle [R, S] \rangle|, \quad (1)$$

where $\langle \cdot | \cdot \rangle$ is the expectation value. The relation implies that it is impossible to simultaneously measure exactly a pair of incompatible (noncommutative) observables.

In the context of both classical and quantum information sciences, it is more natural to use entropy to quantify uncertainties [3, 4]. The first entropic uncertainty relation for position and momentum was given in [5] (which can be shown to be equivalent to Heisenberg's original relation). Later Deutsch [6] found an entropic uncertainty relation for any pair of observables. An improvement of Deutsch's entropic uncertainty relation was subsequently conjectured by Kraus [7] and later proved by Maassen and Uffink [8] (we use base 2 log throughout this paper),

$$H(R) + H(S) \geq \log \frac{1}{c_1}, \quad (2)$$

where $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ are two orthonormal bases on d -dimensional Hilbert space \mathcal{H}_A , and $H(R) = -\sum_j p_j \log p_j$ is the Shannon entropy of the probability distribution $\{p_j = \langle u_j | \rho_A | u_j \rangle\}$ for state ρ_A of \mathcal{H}_A (similarly for $H(S)$ and $\{q_k = \langle v_k | \rho_A | v_k \rangle\}$). The number c_1 is the largest overlap among all $c_{jk} = |\langle u_j | v_k \rangle|^2$ (≤ 1) between the projective measurements R and S .

One of the important recent advances on uncertainty relations is to allow the measured quantum system to be correlated with its environment in a non-classical way, for instance, picking up quantum correlations such as entanglement in quantum cryptography. Historically, the entropic uncertainty relations have inspired initial formulation of quantum cryptography. But the uncertainty relations in the absence of quantum memory did not leave any chance for an eavesdropper to have access to the quantum correlations. Therefore the "classical" uncertainty relations without quantum side information cannot be utilized to improve cryptographic security directly. Berta *et al.* [9] bridged the gap between cryptographic scenarios and the uncertainty principle, and derived this landmark uncertainty relation for measurements R and S in the presence of quantum memory B :

$$H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + H(A|B), \quad (3)$$

* Corresponding Author: jing@ncsu.edu

where $H(R|B) = H(\rho_{RB}) - H(\rho_B)$ is the conditional entropy with $\rho_{RB} = \sum_j (|u_j\rangle\langle u_j| \otimes I)(\rho_{AB})(|u_j\rangle\langle u_j| \otimes I)$ (similarly for $H(S|B)$), and d is the dimension of the subsystem A . The term $H(A|B) = H(\rho_{AB}) - H(\rho_B)$ appearing on the right-hand side is related to the entanglement between the measured particle A and the quantum memory B .

The bound of Berta *et al.* has recently been upgraded by Coles and Piani [10], who have shown a remarkable bound in the presence of quantum memory

$$H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + H(A|B), \quad (4)$$

where c_2 is the second largest overlap among all c_{jk} (counting multiplicity) and other notations are the same as in Eq.(2). As $1 \geq c_1 \geq c_2$, the second term in Eq.(4) shows that the uncertainties depend on more detailed information of the transition matrix or overlaps between the two bases. The Coles-Piani bound offers a strictly tighter bound than the bound of Berta *et al.* as long as $1 > c_1 > c_2$. The goal of this paper is to report a more general and tighter bound for the entropic uncertainty relation with quantum side information.

As reported in [11], there are some examples where the bounds such as B_{Maj} and B_{RPZ} based on majorization approach outperform the degenerate form of Coles and Piani's new bound in the special case when quantum memory is absent. However, it is unknown if these bounds and their approaches can be extended to allow for quantum side information (cf. [4]). Therefore Coles and Piani's remarkable bound Eq. (4) is still the strongest lower bound for the entropic sum in the presence of quantum memory *up to now*. In this paper, we improve the bound of Coles and Piani in the most general situation with quantum memory. Moreover, our new general bound is proven stronger by rigorous mathematical arguments.

To state our result, we first recall the majorization relation between two probability distributions $P = (p_1, \dots, p_d)$, $Q = (q_1, \dots, q_d)$. The partial order $P \prec Q$ means that $\sum_{j=1}^i p_j^\downarrow \leq \sum_{j=1}^i q_j^\downarrow$ for all $i = 1, \dots, d$. Here \downarrow denotes rearranging the components of p or q in descending order. Any probability distribution vector P is bounded by $(\frac{1}{d}, \dots, \frac{1}{d}) \prec P \prec (1, 0, \dots, 0) = \{1\}$. For any two probability distributions $P = (p_j)$ and $Q = (q_k)$ corresponding to measurements R and S of the state ρ , there is a state-independent bound of direct-sum majorization [11]: $P \oplus Q \prec \{1\} \oplus W$, where $P \oplus Q = (p_1, \dots, p_d, q_1, \dots, q_d)$ and $W = (s_1, s_2 - s_1, \dots, s_d - s_{d-1})$ is a special probability distribution vector defined exclusively by the overlap matrix related to R and S . Let $U = (\langle u_j | v_k \rangle)_{jk}$ be the overlap matrix between the two bases given by R and S , and define the subset $\text{Sub}(U, k)$ to be the collection of all size $r \times s$ submatrices M such that $r + s = k + 1$. Following [11, 12] we define $s_k = \max\{\|M\| : M \in \text{Sub}(U, k)\}$, where $\|M\|$ is the maximal singular value of M . Denote the sum of the largest k terms in $\{1\} \oplus W$ as $\Omega_k = 1 + s_{k-1}$ and the i -th largest overlap among c_{jk} 's as c_i . Meanwhile $s_0 = 0$, $s_1 = \sqrt{c_1}$ and $s_d = 1$. It follows from the basic definitions of Ω_k that the following inequalities hold

$$1 = \Omega_1 \leq \Omega_2 \leq \dots \leq \Omega_{d+1} = \dots = \Omega_{2d} = 2,$$

where we noted that $\Omega_2 = 1 + \sqrt{c_1}$.

Our main result is the following entropic uncertainty relation that, much like Coles-Piani's bound, accounts for the possible use of a quantum side information due to the entanglement between the measured particle and quantum memory. For a bipartite quantum state ρ_{AB} on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, we still use H to denote the von Neumann entropy, $H(\rho_{AB}) = -\text{Tr}(\rho_{AB} \log \rho_{AB})$.

Theorem. Let $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ be arbitrary orthonormal bases of the d -dimensional subsystem A of a bipartite state ρ_{AB} . Then we have that

$$H(R|B) + H(S|B) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + \frac{2 - \Omega_4}{2} \log \frac{c_2}{c_3} + \dots + \frac{2 - \Omega_{2(d-1)}}{2} \log \frac{c_{d-1}}{c_d} + H(A|B), \quad (5)$$

where $H(R|B) = H(\rho_{RB}) - H(\rho_B)$ is the conditional entropy with $\rho_{RB} = \sum_j (|u_j\rangle\langle u_j| \otimes I)(\rho_{AB})(|u_j\rangle\langle u_j| \otimes I)$ (similarly for $H(S|B)$), and $H(A|B) = H(\rho_{AB}) - H(\rho_B)$.

We remark that due to $\Omega_{d+1} = \dots = \Omega_{2d} = 2$, the last (non-zero) term of formula (17) can be fine-tuned according to the parity of d . If $d = 2n$, it is $\frac{2 - \Omega_d}{2} \log \frac{c_n}{c_{n+1}}$; if $d = 2n + 1$, it is $\frac{2 - \Omega_{d-1}}{2} \log \frac{c_n}{c_{n+1}}$.

Proof. For completeness we start from the derivation of the Coles-Piani inequality. Observe that the quantum channel $\rho \rightarrow \rho_{SB}$ is in fact $\rho_{SB} = \sum_k |v_k\rangle\langle v_k| \otimes \text{Tr}_A(|v_k\rangle\langle v_k| \otimes I) \rho_{AB}$. As the relative entropy $D(\rho||\sigma) = \text{Tr}(\rho \log \rho) -$

$\text{Tr}(\rho \log \sigma)$ is monotonic under a quantum channel it follows that

$$\begin{aligned}
& H(S|B) - H(A|B) \\
&= D(\rho_{AB} \| \sum_k (|v_k\rangle\langle v_k| \otimes I) |\rho_{AB}(|v_k\rangle\langle v_k| \otimes I)) \\
&\geq D(\rho_{RB} \| \sum_{j,k} c_{jk} |u_j\rangle\langle u_j| \otimes \text{Tr}_A(|v_k\rangle\langle v_k| \otimes I) \rho_{AB}) \\
&\geq D(\rho_{RB} \| \sum_j \max_k c_{jk} |u_j\rangle\langle u_j| \otimes \rho_B) \\
&= -H(R|B) - \sum_j p_j \log \max_k c_{jk},
\end{aligned} \tag{6}$$

where the first expression of Eq. (6) is a basic identity of the quantum relative entropy (cf. [13, 14]). So the state-dependent bound under a quantum memory follows:

$$H(R|B) + H(S|B) \geq H(A|B) - \sum_j p_j \log \max_k c_{jk}. \tag{7}$$

Interchanging R and S we also have

$$H(R|B) + H(S|B) \geq H(A|B) - \sum_k q_k \log \max_j c_{jk}. \tag{8}$$

We arrange the numbers $\max_k c_{jk}$, $j = 1, \dots, d$, in descending order:

$$\max_k c_{j_1 k} \geq \max_k c_{j_2 k} \geq \dots \geq \max_k c_{j_d k}, \tag{9}$$

where $j_1 j_2 \dots j_d$ is a permutation of $1 2 \dots d$. Clearly $c_1 = \max_k c_{j_1 k}$ and in general $c_i \geq \max_k c_{j_i k}$ for all i . Therefore

$$\begin{aligned}
& -\sum_{j=1}^d p_j \log \max_k c_{jk} = -\sum_{i=1}^d p_{j_i} \log \max_k c_{j_i k} \\
& \geq -p_{j_1} \log c_1 - p_{j_2} \log c_2 - \dots - p_{j_d} \log c_d \\
& = -(1 - p_{j_2} - \dots - p_{j_d}) \log c_1 - p_{j_2} \log c_2 - \dots - p_{j_d} \log c_d \\
& = -\log c_1 + p_{j_2} \log \frac{c_1}{c_2} + \dots + p_{j_d} \log \frac{c_1}{c_d}.
\end{aligned} \tag{10}$$

Similarly we also have

$$-\sum_k q_k \log \max_j c_{jk} \geq -\log c_1 + q_{k_2} \log \frac{c_1}{c_2} + \dots + q_{k_d} \log \frac{c_1}{c_d}, \tag{11}$$

for some permutation $k_1 k_2 \dots k_d$ of $1 2 \dots d$. Taking the average of Eq. (7) and Eq. (8) and plugging in Eqs. (10)-(11) we have that

$$H(R|B) + H(S|B) \geq H(A|B) + \log \frac{1}{c_1} + \frac{p_{j_2} + q_{k_2}}{2} \log \frac{c_1}{c_2} + \dots + \frac{p_{j_d} + q_{k_d}}{2} \log \frac{c_1}{c_d}. \tag{12}$$

Using $p_{j_2} + q_{k_2} = \sum_{i=2}^d (p_{j_i} + q_{k_i}) - \sum_{i=3}^d (p_{j_i} + q_{k_i})$ we see that Eq. (12) can be written equivalently as

$$H(R|B) + H(S|B) \geq H(A|B) + \log \frac{1}{c_1} + \frac{1}{2} \sum_{i=2}^d (p_{j_i} + q_{k_i}) \log \frac{c_1}{c_2} + \frac{p_{j_3} + q_{k_3}}{2} \log \frac{c_2}{c_3} + \dots + \frac{p_{j_d} + q_{k_d}}{2} \log \frac{c_2}{c_d}. \tag{13}$$

The above transformation from Eq.(12) to Eq.(13) adds all later coefficients of $\log \frac{c_1}{c_3}, \dots, \log \frac{c_1}{c_d}$ into that of $\log \frac{c_1}{c_2}$ and modify the argument of each log to $\log \frac{c_2}{c_3}, \dots, \log \frac{c_2}{c_d}$. Continuing in this way, we can write Eq.(13) equivalently as

$$\begin{aligned}
& H(R|B) + H(S|B) \\
&= H(A|B) - \log c_1 + \frac{2 - (p_{j_1} + q_{k_1})}{2} \log \frac{c_1}{c_2} + \frac{2 - (p_{j_1} + q_{k_1} + p_{j_2} + q_{k_2})}{2} \log \frac{c_2}{c_3} + \dots + \frac{2 - \sum_{i=1}^{d-1} (p_{j_i} + q_{k_i})}{2} \log \frac{c_{d-1}}{c_d}.
\end{aligned} \tag{14}$$

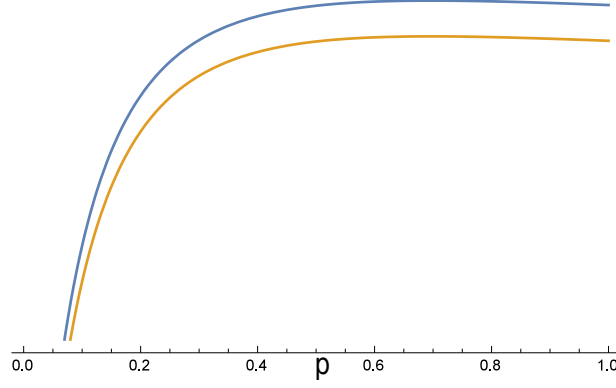


FIG. 1: Comparison of bounds for entangled ρ_{AB} . The upper blue curve is the new bound (5) and the lower yellow curve is Coles-Piani's bound.

Since $P \oplus Q \prec \{1\} \oplus W$, we have $p_{j_1} + q_{k_1} \leq \Omega_2, \dots, p_{j_1} + q_{k_1} + \dots + p_{j_{d-1}} + q_{k_{d-1}} \leq \Omega_{2(d-1)}$. Plugging these into Eq.(12) completes the proof. ■

We remark that our newly constructed bound is stronger than Coles-Piani's bound in all cases except when the observables are mutually unbiased (i.e. $c_{jk} = |\langle u_j | v_k \rangle|^2 = 1/d$ for any j, k).

As an example, consider the following 2×4 bipartite state,

$$\rho_{AB} = \frac{1}{1+7p} \begin{pmatrix} p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & 0 & 0 & 0 & p \\ 0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+p}{2} & 0 & 0 & \frac{\sqrt{1-p^2}}{2} \\ p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & \frac{\sqrt{1-p^2}}{2} & 0 & 0 & \frac{1+p}{2} \end{pmatrix}, \quad (15)$$

which is known to be entangled for $0 < p < 1$ [15]. We take system A as the quantum memory, consider the following two projective measurements: $\{|v_k\rangle\}$ are the standard orthonormal basis on \mathcal{H}_B and $\{|u_j\rangle\}$ are given by

$$\begin{aligned} |u_1\rangle &= \left(\frac{12}{\sqrt{205}}, \frac{6}{\sqrt{205}}, \frac{4}{\sqrt{205}}, \frac{3}{\sqrt{205}} \right)^T, \\ |u_2\rangle &= \left(-\frac{66}{29\sqrt{205}}, \frac{172}{29\sqrt{205}}, \frac{183}{29\sqrt{205}}, -\frac{324}{29\sqrt{205}} \right)^T, \\ |u_3\rangle &= \left(-\frac{11}{29\sqrt{298}}, \frac{309}{29\sqrt{298}}, -\frac{195\sqrt{\frac{2}{149}}}{29}, -\frac{27\sqrt{\frac{2}{149}}}{29} \right)^T, \\ |u_4\rangle &= \left(\frac{9}{\sqrt{298}}, -\frac{9}{\sqrt{298}}, -3\sqrt{\frac{2}{149}}, -5\sqrt{\frac{2}{149}} \right)^T. \end{aligned}$$

Then the overlap matrix $(|\langle u_j | v_k \rangle|^2)_{jk}$ is given by

$$\begin{pmatrix} \frac{144}{205} & \frac{36}{205} & \frac{16}{205} & \frac{9}{205} \\ \frac{4356}{172405} & \frac{29584}{172405} & \frac{33489}{172405} & \frac{104976}{172405} \\ \frac{121}{250618} & \frac{95481}{250618} & \frac{76050}{125309} & \frac{1458}{125309} \\ \frac{81}{298} & \frac{81}{298} & \frac{18}{149} & \frac{50}{149} \end{pmatrix}. \quad (16)$$

Thus $\Omega_4 \neq 2$ and $c_2 \neq c_3$. The comparison between Coles-Piani's bound and Eq. (5) in the presence of quantum memory is displayed in FIG. 1, which shows that our new bound is strictly tighter for all $p \in (0, 1)$.

After presenting the general result, we now turn to its special situation for the state-independent bound in the absence of quantum memory. As many state-independent bounds cannot be generalized to the general situation, a separate treatment is needed and one will see that our new bound fares reasonably well even in the absence of quantum memory.

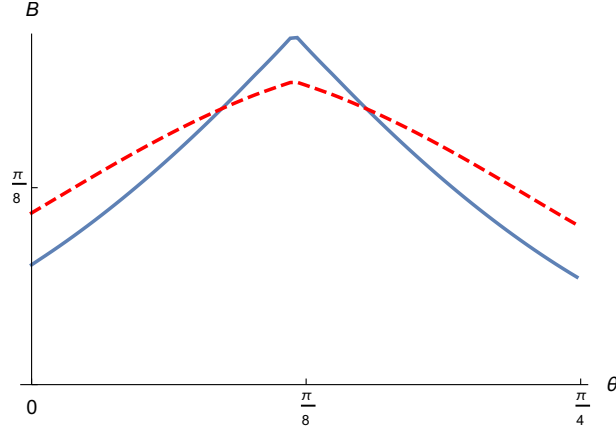


FIG. 2: Comparison of direct-sum majorization bound (dashed red) and Eq. (17) for unitary matrices $U(\theta)$.

Corollary. Let $R = \{|u_j\rangle\}$ and $S = \{|v_k\rangle\}$ be any two orthonormal bases on d -dimensional Hilbert space \mathcal{H}_A . Then for any state ρ_A over \mathcal{H}_A , we have the following inequality:

$$H(R) + H(S) \geq \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2} + \frac{2 - \Omega_4}{2} \log \frac{c_2}{c_3} + \frac{2 - \Omega_6}{2} \log \frac{c_3}{c_4} + \cdots + \frac{2 - \Omega_{2(d-1)}}{2} \log \frac{c_{d-1}}{c_d}, \quad (17)$$

where Ω_k and c_i are defined in Eq.(5).

The corollary can be similarly proved due to the following simple observation. When measurements are performed on system A , $H(R) + H(S) \geq -\sum_j p_j \log \sum_k q_k c_{jk} + H(A) \geq -\sum_j p_j \log \max_k c_{jk} + H(A)$. Then the corollary follows directly from the proof of the theorem.

We now compare our bound given in the corollary with some of the well-known bounds in this special case. First of all, our new bound is clearly tighter than Coles-Piani's bound $B_{CP} = \log \frac{1}{c_1} + \frac{1 - \sqrt{c_1}}{2} \log \frac{c_1}{c_2}$ as we have already shown mathematically. In [11] Rudnicki *et al.* obtained the *direct-sum majorization* bound, one of the major ones for the state-independent states, thus we will focus on comparing our bound with this one. Consider the following unitary matrices between two measurements

$$U(\theta) = M(\theta)OM(\theta)^\dagger, \quad (18)$$

where $\theta \in [0, \pi/4]$ and

$$M(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta_1 & \sin \theta_1 \\ 0 & -\sin \theta_1 & \cos \theta_1 \end{pmatrix}, \quad (19)$$

with the overlap matrix

$$O = \begin{pmatrix} 0.4575 & 0.4575 & 0.7625 \\ -0.2453 & 0.8892 & -0.3863 \\ -0.8547 & -0.0103 & 0.5190 \end{pmatrix}. \quad (20)$$

FIG. 2 shows that the direct-sum majorization bound and our bound Eq. (17) are complementary, as there are regions where our bound is tighter. This implies that our bound in this special case is also nontrivial. We would like to remark that there are other bounds for the entropic uncertainty relations in the absence of quantum side information, but most of them cannot be generalized to the case with quantum memory.

Note that the overlaps, which are commonly used in entropic uncertainty relations, are state-independent measurements so we can only consider them when the experimental device is trusted. For *device-independent uncertainty* based on state-dependent and incompatible measures, see [16]. There seems no clear relation between our bound and the bound based on state-dependent anticommutators, and it is still open whether the approach of [16] based on state-dependent measurements can be extended to allow for the quantum side information. On the other hand, our result holds for the general case with the quantum side information.

Conclusion. We have found new lower bounds for the sum of the entropic uncertainties in the presence of quantum memory. Our new bounds have formulated the complete dependence on all d largest entries in the overlap matrix

between two measurements on a d -dimensional Hilbert space, while the previously best-known bound involves with the first two largest entries. We have shown that our bounds are strictly tighter than previously known entropic uncertainty bounds with quantum side information by mathematical argument in the general situation. In the special case without quantum memory, our bound also offers significant new information as it is complementary to some of the best known bounds in this situation. Moreover, as entropic uncertainty relations in the presence of quantum memory have a wide range of applications, our results are expected to shed new lights on investigation of quantum information processing such as information exclusive relation [17], entanglement detection, quantum key distribution and other cryptographic scenarios.

Acknowledgments The work is supported by NSFC (grant Nos. 11271138, 11531004, 11275131G?11675113), CSC and Simons Foundation grant 198129.

-
- [1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
 - [2] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
 - [3] I. Białynicki-Birula and L. Rudnicki, Statistical Complexity, ed. by K. Sen, Springer Netherlands, Dordrecht pp. 1-34 (2011).
 - [4] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, arXiv: 1511.04857v1.
 - [5] I. Białynicki-Birula and J. Mycielski, Comm. Math. Phys. **44**, 129 (1975).
 - [6] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
 - [7] K. Kraus, Phys. Rev. D. **35**, 3070 (1987).
 - [8] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
 - [9] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
 - [10] P. J. Coles and M. Piani, Phys. Rev. A **89**, 022112 (2014).
 - [11] L. Rudnicki, Z. Puchała, and K. Życzkowski, Phys. Rev. A **89**, 052115 (2014).
 - [12] Z. Puchała, L. Rudnicki, and K. Życzkowski, J. Phys. A **46**, 272002 (2013).
 - [13] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **83**, 062338 (2011).
 - [14] P. J. Coles, Phys. Rev. A **85**, 042103 (2012).
 - [15] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
 - [16] J. Kaniewski, M. Tomamichel, and S. Wehner, Phys. Rev. A **90**, 012332 (2014).
 - [17] Y. Xiao, N. Jing, and X. Li-Jost, Sci. Rep. **6**, 30440 (2016).